

IT Forensics Assignment

<Windows Registry>

Jordan Forde C14403588

School of Computing
Dublin Institute of Technology

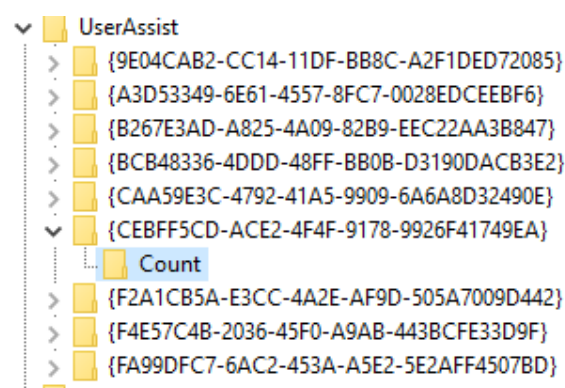
<07/11/2017>




<DT228, Computer Science/2017>

Table of Contents:

Cover Page.....	1
Table of Contents.....	2
Question 1 User Assist.....	3
Question 2 USB Devices.....	4
Question 3 Jump Lists.....	5
Question 4 WIFI networks.....	6
Question 5 Hiding data in the Registry.....	7
Appendices.....	8
References.....	10

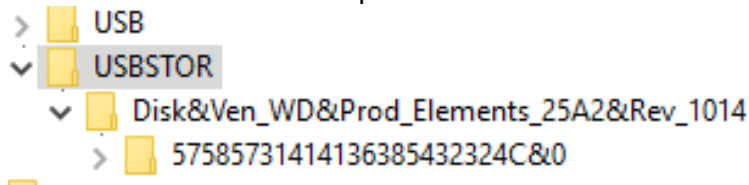
1. The Windows registry is a database in the Windows operation system that contains information about each user of the system. This information can include software programs and hardware devices. The Forensic information that can found in the windows registry can provide a substantial amount of valuable data that can show who, what, when are where something took place on the system. In some case the actions that are performed on the system can provide the missing link in the case. The information the in the registry also includes the last time the user was logged on to the system. The registry will also show any devices that have been inserted into the machine including mouse, printers and headphones, anything that is external to the machine. With the registry, we can also see a list of what wireless networks the system has been connected to. This information can tell us where the user has been. All this information can be substantial evidence in a case against someone. One of the biggest advantage of what we can see is what files were accessed by a user. Much like a user logging onto the system we can see what files were accessed and when they were accessed. The folder CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} \Count in the UserAssist key shows us the recently ran executable files. The registry is encrypted in rot13, so we must decrypt it to see what files have been accessed. We can see this in the [Appendices \[1\]](#). We can see what files I have accessed on my system in pictures below.



 {6Q809377-6NS0-4440-8957-N3773S02200R}\AIVQVN Pbecbengyba\Pbageby Cnary Pyvrag\aipcyhv.rkr
 {6Q809377-6NS0-4440-8957-N3773S02200R}\Fhoyvzr Grkg 3\fhoyvzr_grkg.rkr
 {6Q809377-6NS0-4440-8957-N3773S02200R}\Pbzzba Svyrf\zvpebfbg funerq\PyvpxGbEha\BssvprP2EPyvrag.rkr

The highlighted file is the one I decrypted, and it was to sublime_text.exe. CCleaner is a piece of software which cleans out all the temporary files that you have gathered over time. Some programs leave files behind that take up space and cause pop-ups, we can use CCleaner to clear them out. CCleaner will also clear out your browsing history and temporary internet files. Using CCleaner is very good for your computer as computers can fill up with cache data and temporary files. A person could clean out their system once a week but if someone is being investigated and they see that the suspect just downloads CCleaner and ran It for the first time it can be very suspicious. Below we can see CCleaner after being ran in the [Appendices \[2\]](#) this will tell you what files have been thrown out.

- The location of USB devices, that have been connected to the system, in the windows registry is HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Enum\USBSTOR. This location stores information about the device when it is plugged into the system. It stores information such as serial number or friendly name. Below we can see a picture of this location and the device.



As we can see from this picture this is the only device which has been connect to my machine. This device is an external 500GB hard drive. The serial number can be seen under the devices name '57585731414136385432324C&0'. If we click into this serial number, we are given the following information

(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x0000000b (11)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{22220a3f-a1af-5a9d-85a0-1be4e19c14bf}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0003
FriendlyName	REG_SZ	WD Elements 25A2 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskWD____Elements_25A2____1014 USBSTOR\DiskWD____Elements_25A2____ USBSTO
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

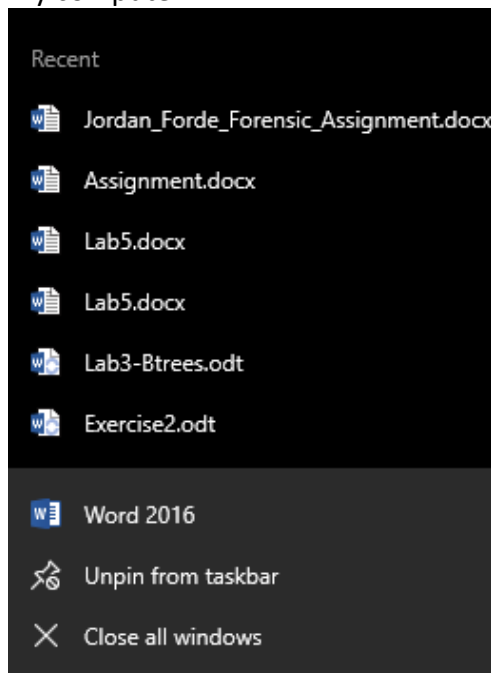
As we can see from the picture above friendly name on this device WD Elements 25A2 USB Device. Friendly names are names given to a device so humans can read what the device is and what its used for without looking at numbers. To see the last, write time of this USB device we export the folder with the devices serial number as a .txt and open it. We can see by the picture below in the [Appendices \[3\]](#) the last write time was the 22nd of October at half five. To find the volume name of the device we first must go to the USB folder one directory up from USBTOR and find the devices serial number among the folders. The next step is to the directory HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows Portable Devices\Devices\ here is where we can find the devices volume number and as we can see by the picture below in [Appendices \[4\]](#) the name is STORAGE. I couldn't find the volume serial number on my device. I have found articles online to suggest the function ready boost on the USB devices inhibits the volume serial number. What ready boost does is it uses a USB device as extra memory to increases the performance.

3. A jump list is a feature brought in to windows 7 which gives the user a list of recently accessed files in a specific application. This feature gives a graphical list of the recent items that were opened in that application. This jump list will show the date and time the file was last accessed and give us the size of the file and much more. The jump list information is stored in the folder C:\Users\[User Profile]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations. These files are created when a user opens a file or access an application. However, if we go to a different folder in the same directory called /CustomDestinations this contains the same information but to applications that are pinned to a user's start menu or task bar. Below we can see a picture of my CustomDestinations directory.

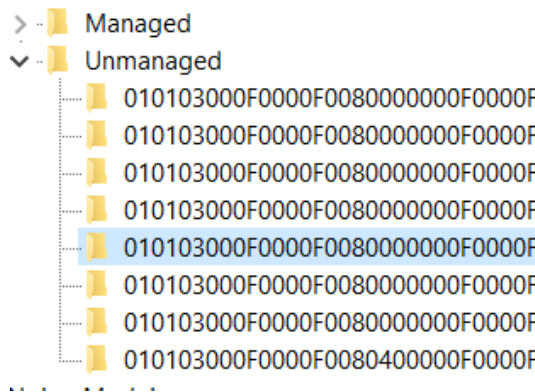
This PC > Local Disk (C:) > Users > jorda > AppData > Roaming > Microsoft > Windows > Recent Items

Name	Date modified	Type	Size
5d696d521de238c3.customDestinations-ms	21/10/2017 20:52	CUSTOMDESTINA...	4 KB
9d1f905ce5044aee.customDestinations-ms	21/10/2017 20:52	CUSTOMDESTINA...	2 KB
59fe1486d27aa9d0.customDestinations-ms	22/10/2017 11:24	CUSTOMDESTINA...	4 KB
ec3e36af0cdcb3e1.customDestinations-ms	22/10/2017 11:25	CUSTOMDESTINA...	7 KB
f18460fdded109990.customDestinations-ms	22/10/2017 14:22	CUSTOMDESTINA...	1 KB

There is a potential for some source of forensic information to be gathered using jump lists, however a user can turn off the service if the wish. A jump list tracks files that are used by a specific user on the system, so this means we can see where the most activity is on the system. A forensic examiner can learn a lot of information from a jump list like what habits the user has on the system and what sort of applications are run on them. Below is an example of a jump list on my computer.



- The wireless network information that is gathered when a machine connects to a network is located in the windows registry in the folders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures. The folder below shows a list of WIFI networks that I have connected to on my machine.



The WIFI network that is highlighted in the above picture is my mobile phones hot spot. The registry has stored information about my phone witch you can see in the picture below.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	94 65 2d 6e d6 7a
Description	REG_SZ	OnePlus 5
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	OnePlus 5
ProfileGuid	REG_SZ	{959F84CE-3378-4973-ACE6-8C58B9ED232E}
Source	REG_DWORD	0x00000008 (8)

This key contains different information the first being the MAC address which is used to uniquely identify the hardware. We then see the description witch in my case is the name of my phone OnePlus 5. We then see there is no DnsSuffix assigned to the network. If we look at picture below in the [Appendices \[5\]](#) we can see the DIT WIFI and its DnsSuffix is ict.ad.dit.ie. The ProfileGuid is assigned in the registry. We can use this GUID to find the registry key containing the IP address.

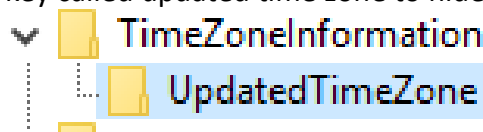
The following is a list of wife networks and their mac address I have been connected to:

WIFI: Central Library MAC Address: 00 18 0a 11 ca 50
WIFI: Vodafone-D4D0 MAC Address: 0c d6 bd d0 d4 d0
WIFI: eircom60463439 MAC Address: ec 43 f6 42 6a b0
WIFI: eir09753822 MAC Address: 84 be 52 96ae b1

5. Yes, it is possible to hide information in the windows registry. There are many ways to hide information in the windows registry but the most well-known way to hide the data is in the directory `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`. The `TimeZoneInformation` key stores information of your PC's local Time. This key has two entities inside it which can store data such as strings or binary data. Both entities are not used by windows and could be left empty or could be filled with information you don't want anyone to see. Why we would use these entities is that if we were to change another key somewhere else it could affect the system in such a way where it could never be used again or cause serious damage. As these entities are not used by windows it will not affect the system. The names of these entities are `StandardName` and `DaylightName`. As we can see from the picture below the `DaylightName` data has been changed to a password this is an example of some of the information you may hide.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xffffffff (4294967236)
Bias	REG_DWORD	0x00000000 (0)
DaylightBias	REG_DWORD	0xffffffff (4294967236)
DaylightName	REG_SZ	Password: pass123
DaylightStart	REG_BINARY	00 00 03 00 05 00 01 00 00 00 00 (
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-262
StandardStart	REG_BINARY	00 00 0a 00 05 00 02 00 00 00 00 (
TimeZoneKeyName	REG_SZ	GMT Standard Time

Another way to hide date in a similar way is to create a new key under TimeZoneInformation or anywhere in the registry. We can call this new key anything but to make it less suspicious it should have a name related to the keys that surround it to mislead anyone trying to find our hidden date. In this new key, we can create as many entities as we want to hide our data. I created a new key called updated time zone to hide my data.



In this key, we have hidden data in our fake key. We have both String and binary data. The content of the string entity BankDetails is the card number of the user. The binary data entity AccountDetails has some data inserted in it.

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 BankDetails	REG_SZ	CardNumber: 1234
 AccountDetails	REG_BINARY	11 10 01 10 10 10 10

Appendices:

[1]:

```
Fhoyvzr Grkg 3\fhoyvzr_grkg.rkr
```

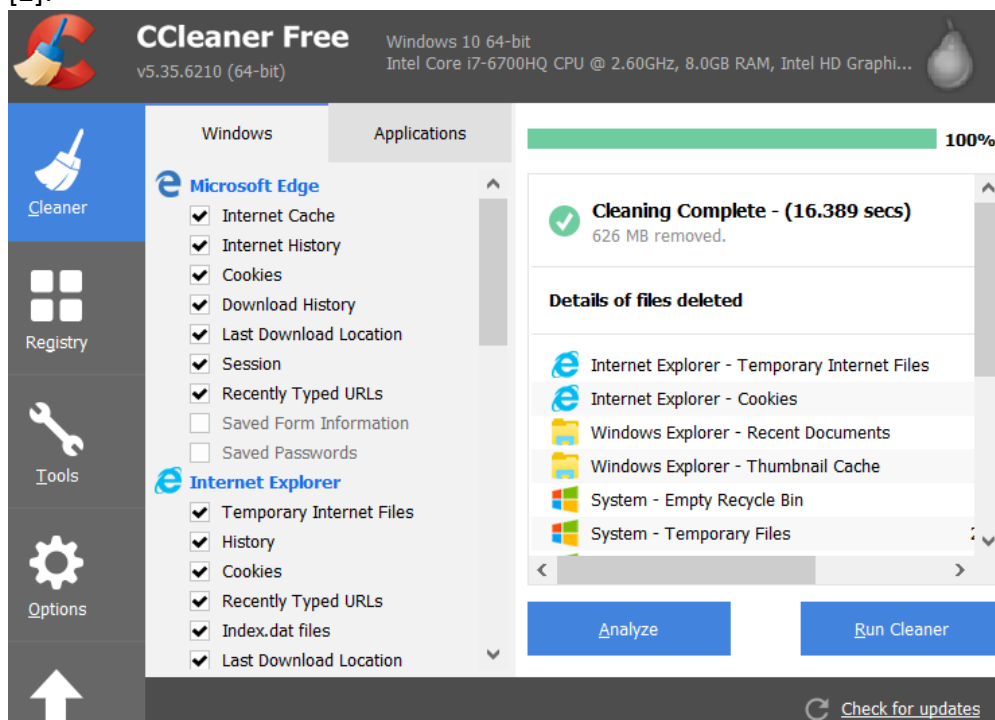


ROT13 ▾



```
Sublime Text 3\sublime_text.exe
```

[2]:



[3]:

Key Name: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_WD&Prod_Elements_25A2&Rev_1014\5
 Class Name: <NO CLASS>
 Last Write Time: 22/10/2017 - 17:24

[4]:

Windows Portable Devices		
Devices		
SWD#WPDBUSENUM#{88CCC1B	(Default)	REG_SZ (value not set)
SWD#WPDBUSENUM#{B6D5C64	FriendlyName	REG_SZ STORAGE

[5]:

(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	00 04 96 2e 84 d0
Description	REG_SZ	ditwifi
DnsSuffix	REG_SZ	ict.ad.dit.ie
FirstNetwork	REG_SZ	ditwifi
ProfileGuid	REG_SZ	{B56CC438-2CA5-48A7-B0AA-9B93687510FD}
Source	REG_DWORD	0x00000008 (8)

References:

Question 1:

<http://www.rot13.com/>

<https://www.hackers-arise.com/single-post/2016/10/21/Digital-Forensics-Part-5-Analyzing-the-Windows-Registry-for-Evidence>

<https://www.piriform.com/docs/ccleaner/introducing-ccleaner/what-is-ccleaner>

Question 2:

<https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/>

http://www.forensicswiki.org/wiki/USB_History_Viewing

<http://hatsoffsecurity.com/2014/06/08/usb-forensics-pt-4-volume-serial-number/>

Question 3:

<https://articles.forensicfocus.com/2012/10/30/forensic-analysis-of-windows-7-jump-lists/>

https://www.nirsoft.net/utils/jump_lists_view.html

<https://www.blackbagtech.com/blog/2017/01/12/windows-10-jump-list-forensics/>

Question 4:

<https://www.sans.org/reading-room/whitepapers/compliance/wireless-networks-windows-registry-computer-been-33659>

Question 5:

<http://www.darknessgate.com/security-tutorials/date-hiding/hiding-data-in-registry/>